

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

11/12/2010

SUBJECT:

Multiple Vulnerabilities in Apple Mac OS X Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been identified in Apple Mac OS X and Apple Mac OS X Server. These vulnerabilities may be exploited if a user visits, or is redirected to a web page or opens a malicious file that was designed to take advantage of these vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Apple Mac OS X Server 10.5 – 10.5.8
- Apple Mac OS X Server 10.6 – 10.6.4
- Apple Mac OS X 10.5 – 10.5.8
- Apple Mac OS X 10.6 – 10.6.4

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Universities/Schools: High

Home users: High

DESCRIPTION:

Thirty-five vulnerabilities have been identified in Apple Mac OS X and Mac OS X Server. These vulnerabilities may be exploited if a user visits, or is redirected to a web page or opens a malicious file that was designed to take advantage of these vulnerabilities.

The following vulnerabilities were identified by Apple:

- A denial-of-service vulnerability affecting the Apple Filing Protocol (AFP) component exists when handling reconnection network packets.
- A directory-traversal vulnerability affecting the AFP server component which may allow authenticated users to create files outside of a file share. An attacker can exploit this issue to execute arbitrary code.

- A security vulnerability that affects the AFP Server component which may allow attackers to determine the existence of an AFP share with a given name.
- A buffer-overflow vulnerability exists in the AppKit component. This issue may be exploited if string containing bidirectional text is rendered and is translated with an ellipsis resulting in an attacker executing arbitrary code.
- A buffer-overflow vulnerability affecting the Apple Type Services (ATS) when handling embedded fonts with long names.
- A stack-based buffer overflow vulnerability exists in the Apple Type Services (ATS) when handling embedded fonts. An attacker can exploit this issue to execute arbitrary code.
- A memory corruption issue affecting the Apple Type Services (ATS) exists when handling embedded fonts. This vulnerability could result in an attacker executing arbitrary code.
- A security vulnerability affecting the CFNetwork component when handling domain applications in cookies.
- A stack-based buffer overflow and a memory corruption vulnerability exists in the CoreText component when handling a PDF file. An attacker can exploit this issue to execute arbitrary code.
- A local security-bypass vulnerability affecting the Directory Service component which may allow attackers to bypass the password validation service.
- A stack-based buffer overflow vulnerability affecting the Directory Service component when handling large passwords resulting arbitrary code execution.
- A memory corruption vulnerability impacts the Directory Service component when handling a Universal Disk Image Format (UDIF) disk image. An attacker can exploit this issue to execute arbitrary code.
- An unbounded memory corruption vulnerability that affects the Image Capture component when handling specially crafted image files allowing attackers to execute arbitrary code.
- Multiple memory corruption issues exist in ImageIO when handling Photoshop Data (PSD) images which may allow attackers to execute arbitrary code on affected systems.
- A heap-based buffer overflow vulnerability affecting the Image RAW component exists when a user opens a specially crafted RAW image file. An attacker can exploit this issue to execute arbitrary code.
- A local denial-of-service vulnerability affecting the Kernel component which may allow an attacker to crash a system.
- A denial-of-service vulnerability affecting the Networking component exists when handling Protocol Independent Multicast (PIM) packets.
- A spoofing vulnerability exists in the OpenSSL component allowing a remote user to bypass certificate validation steps, causing OpenSSL to accept any certificate signed by a trusted root.
- A security bypass vulnerability affecting the Password Server component may allow attackers to login with an expired password.
- A denial-of-service vulnerability affecting the Printing component which may allow an attacker to crash the component.

- Four memory corruption issues and one buffer overflow vulnerability exist in QuickTime when users open specially crafted movie files. This vulnerability could result in an attacker executing arbitrary code.
- Stack-based buffer-overflow and memory corruption vulnerabilities affect the QuickLook component when handling Microsoft Office files and Excel files that may result in an attacker executing arbitrary code.
- Four remote code execution vulnerabilities exist when users open specially crafted FlashPix, GIF or JP2 image files in QuickTime.
- An information-disclosure vulnerability affecting the Safari RSS component when handling a 'feed:' URI.
- The Wiki server is vulnerable to a JavaScript injection.
- An unauthorized access vulnerability affects the Time Machine component.
- A buffer-overflow vulnerability affecting the 'xar' component when extracting a malicious archive may result in an attacker executing arbitrary code.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attempts will result in a denial-of-service.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Apple:

<http://support.apple.com/kb/HT4435>

Secunia:

<http://secunia.com/advisories/42151>

Security Focus:

<http://www.securityfocus.com/bid/44778>

Zero Day Initiative:

<http://www.zerodayinitiative.com/advisories/ZDI-10-248/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1378>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1803>

